November 4, 2010 NIST Smart Grid Privacy Subgroup Meeting Notes

Minutes by Rebecca Herold

Please send this distribution list any necessary corrections or additions.

Next full group teleconference meeting:

Thursday November 11, 2010 at 11:00am edt

Here are my summary notes from the meeting:

TO-DO FOR UTILITIES IN GROUP: Please let the group know what your organizations would think of the technology described in George Danezis' paper, also considering the discussion notes below.

1. Miscellaneous

i. You can see all the past meeting minutes on our privacy twiki:
http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CSCTGPrivacy

ii. There is also a table on the twiki with information about where various members of our group are speaking on Smart Grid privacy.
   a. Send your info to Rebecca to add if it is not there.
   b. Send our group members' names involved, date, location, and URL if available.

2. Team reports

i. Matrix update: Rebecca
   a. Jason P, Tanya and her hope to get it finished next week and distributed to the full group.
   b. The teams should then reference it as they continue with their work.

ii. NSTIC Team update: Amanda Stallings, Ohio PUC (team lead)
   a. Discussing framework from June draft
   b. Taking things slowly until final doc is released
   c. Discussed pilot project proposal and how it relates to NSTIC
   d. Centered on authentication requirements and how it will tie in with utilities web portals
   e. Need to balance usability with security
   f. Will have guest speakers attend from utilities and from the SRI who can give ideas about how their agencies will be affected by the NSTIC initiative
   g. Amanda getting info from Duke Energy to get their perspective
   h. Tentative meeting Friday, 11/12 at 2pm eastern; Peter Neumann will speak.

iii. PEV Team update: Chris Kotting provided in Coop's absence
   a. Is mostly at high level working on getting everyone to have a consistent understanding of the issues.
   b. Still identifying issues to look into further
   c. Will be communicating with the PAP11 team
   d. Calls on Mondays at noon eastern

iv. Third Party Team update: Karen M provided in Brent Struthers' absence
   a. Continuing meetings and identifying issues to address and work on
   b. Still preliminary

v. Privacy Use Cases Team: Christine Hertzog (team lead)
   a. Reviewing existing Chapter 10 use cases in NISTIR 7628
   b. Looking at how to add privacy issues
   c. Will take existing privacy use cases from the privacy chapter of NISTIR, reformat to a more similar structure and looking at how to condense them

d. Looking at ways to incorporate the CPNI principles from the FCC and incorporate them as well
e. Erick and Chris K will talk about this at our full group meeting on Dec 9
f. Will continue approaching the mapping of OECD privacy principles into the existing use cases
g. Meetings occur Thursdays at 10am eastern

3. Guest Speaker

a. Klaus Kursawe introduced his guest, George Danezis from Microsoft Research Cambridge, who discussed his work on developing "a secure protocol between a customer's electricity meter and a utility provider that reveals the total consumption fee, while keeping private the individual measurements."
b. For reference, see the paper Klaus sent on Wednesday, November 3 to this mail list.
c. Here are my notes from George's discussion (NOTE: this is not comprehensive, but hopefully provides a good representation of his talk to accompany the paper):
    i. Working on privacy technology ~10 yrs. Building systems that will not leak personal information. Take systems and try to find ways to do what needs to be done without negative privacy impacts. Applied to a variety of situations and technologies.
    ii. Our NISTIR 7628 chapter provides more information and details about why data is collected, which he likes a lot.
    iii. Key approach to privacy in smart metering when fine-grained collection of data is performed; main issue is association with billing. Addressing assumption that billing requires detailed energy usage data, which it does not.
    iv. Made a generic model of the problem. Made a meter. The data is packaged in a mathematically special way and associated with a type of signature to validate the meter is authentic and not fake.
    v. Take certified meter readings and combine with certified meters to create a certified bill.
    vi. In terms of deployment there are also advantages. The only thing about the meters that will change is how the meters will be certified.
    vii. Using the technology can calculate all bills of all households in UK in 10 days.
    viii. Have not rolled it out on the smart meters itself.
d. Here are my notes from the conversation and discussion following George's initial presentation.
    i. Michelle from the Ontario IPC: Ontario model the govt has taken sends the data to a central govt agency, then it goes to the utilities for billing purposes. In EU she met with some folks to discuss. University of Toronto is working to assist with how the centralization is done, and to look at the value of the data.
    ii. George: UK govt is considering a centralized database approach.
    iii. Michelle: Much of govt utility activity is at the province level.
    iv. George: UK slightly back from Ontario response. Aside from billing what other purposes is the data used for?
    v. Michelle: The central agency is there to ensure consistency and quality control aspects of the meters. Vision is to use the data to see behavioral changes, endless possibilities.
    vi. Klaus: example of other purposes?
    vii. Michelle: That's why University of Toronto is looking at the potentials. Heard that Italy is far ahead, but don't know what they are doing with the data.
    viii. George: Approach with schemes developed: the data is not discarded; it is just not included for billing. Choice of user to log into Google Power Meter or other third party and provide that data to them to receive the additional services. Govts and large utilities don't have a good reputation with holding and using data in good ways. Users making choices about who to provide data to tend to provide the most value. Gov't holding data and having third parties get to it is not typically a good model.
    ix. Gail: Agree individual can most benefit from fine grained data, and being able to choose services. In Jerusalem talked a lot about communities and households with many occupants. Has George or Michelle addressed multiple consents for use of information for all individuals involved?

x. George: Important point. The technology does not address this issue, it just addresses the data involved. If there is a significant technology aspect, e.g., how to allow individuals access meter data, it could be applied. But otherwise this technology doesn't address the issue.
xi. Klaus: Unless you track who is in the house, it is very hard to know who actually is in the house. Perhaps only solution is billing data-free. Perhaps have all potentially involved to provide a consent.
xii. Gail: You've eliminated fine grained billing info and keeping, e.g., landlords from seeing occupants' individual data.
xiii. Does this solution/approach address issues in Netherlands where they have provided rules for what must be followed to implement smart meters?
xiv. Klaus: I would think this would be a good way to address the problem.
xv. George: Issue of Netherlands shows privacy technology can be an enabler of adoption. The decision is that since there was no choice about deploying smart meters it violated privacy. By providing a choice many issues are resolved or at least addressed.
xvi. Gail: Very different from the U.S. How do our utilities feel?
xvii. Amanda: Utility companies use granular data for code enforcement. Would they still have access? Not sure how the time of use rate would be able to be done with such a technology. Price per 15-minute intervals is being planned; how could this be accomplished through these types of technologies?
xviii. George: As long at the utilities advertise what the tariffs are per 15 minute intervals the meter tool can bill based upon these intervals. Considered load balancing, etc. Taking meter readings and taking that output and applying it over aggregated periods of time, rather large or small. For plotting trends, aggregated data can also be used.
xix. Amanda: Can we see a bill example? Before and after?
xx. George: Will provide some more sample material. Have not yet gotten to the bill creation. A work in progress. Will give whenever such info is available.
xxi. Amanda: In Ohio company is required to give customers detailed info, including past reading, accumulated usage, current usage, etc. Talk of being able to see how much energy specific appliances use. Duke is providing rebates on KW hours saved per each event.
xxii. Gail: That is in comparison to Google Power Meter, etc.
xxiii. George: On rebate point, there are extremely fast protocols, but also very flexible techniques for creating bills in arbitrary ways. E.g., charge rates based upon time or appliance/device. Can calculate bills with this device in a privacy friendly way.
xxiv. Tanya: Using algorithms and codes that have gone through the NIST review process?
xxv. George: Depends upon the complexity of the tariff scheme. If only thing done is the simple scenario, they can be done using standard NIST algorithms. If they start using more complex billing policies, then more powerful crypto is needed which has not yet gone through the NIST approval.

4. Other topics: Open floor

a. Brent is working on getting an FBI rep to tentatively speak next week, or at some other upcoming weekly meeting.
b. Rebecca working to get RFID privacy experts from the University of Wollongong in Australia to speak at an upcoming meeting.
c. Gail: Michel Karstens from the Netherlands would be a good guest; will send the report from there in English. Also, as soon as Jules' interview on Smart Grid is published, will give direct URL about it.

Thanks,

Rebecca